

The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, individually on her
own behalf and on behalf of all others similarly
situated,

Plaintiff,

v.

MICROSOFT CORPORATION, a Delaware
corporation,

Defendant.

Case No. 2:11-cv-01438-JCC

**PLAINTIFF'S THIRD AMENDED
CLASS ACTION COMPLAINT**

PLAINTIFF'S THIRD AMENDED CLASS ACTION COMPLAINT

Plaintiff Rebecca Cousineau ("Cousineau" or "Plaintiff") brings this Third Amended Class Action Complaint ("Complaint") against Defendant Microsoft Corporation ("Microsoft" or "Defendant") based upon its practice of unlawfully tracking its users' geolocation information through their mobile devices. Plaintiff, for her Complaint, alleges as follows upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys:

NATURE OF THE ACTION

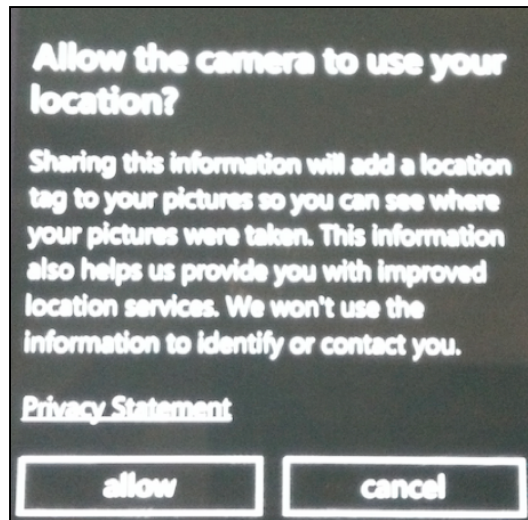
1. Until this lawsuit brought these issues to light, Microsoft intentionally tracked the movements of its users' mobile devices in direct contravention of their privacy settings and the

1 law. While Microsoft claimed that users could opt-out of its location-tracking program,
2 Microsoft designed its mobile device software to deceptively track its users' locations even after
3 they *affirmatively denied* Microsoft consent to do so. As discussed more fully herein, Microsoft
4 effectuated this scheme through its popular mobile operating system ("OS"), Windows Phone 7
5 ("Windows Phone"), which is used by a variety of manufacturers of mobile devices, such as
6 HTC, Samsung, and LG. Regardless of the model of mobile device the software operates on,
7 Microsoft consciously designed its OS to siphon geographic location information from the
8 device revealing the user's specific whereabouts and transmit this data to Microsoft's servers.

9 2. Over the past decade, mobile telephony use among United States consumers has
10 grown exponentially. Seeking to capitalize on this new medium of communication, Microsoft is
11 racing to develop a system that facilitates targeted advertisements to consumers based upon their
12 geographic locations. Before Microsoft is able to execute such a marketing campaign, however,
13 it must first compile data points to create a digital map by collecting geographic information and
14 unique identifiers from cellular towers, wireless network routers, cellular telephones, and
15 computer systems.

16 3. Faced with the expensive and laborious task of collecting this information,
17 Microsoft has elected to gather the necessary geolocation information through its customers'
18 mobile devices. In this way, Microsoft uses its customers as a virtual army of surveyors who
19 constantly gather and transmit the geolocation information necessary to build its digital map.

20 4. One method by which Microsoft gathers such data is through its camera
21 application, which comes standard with a mobile device running the Windows Phone OS. The
22 first time a user opens the camera application, a display screen prompts the user to allow or deny
23 Microsoft access to his or her geolocation:



(The above depiction is a true and accurate copy of the Windows Phone OS display screen (“Display Screen”).)

5. Users who click “cancel” explicitly deny Microsoft access to their geolocations. Unfortunately for its users, however, Microsoft continued to collect users’ location information, regardless of whether or not the individual chose “cancel.” Thus, Microsoft surreptitiously forced even unwilling users into its non-stop geo-tracking program in the interest of developing its digital marketing grid.

6. Microsoft publicly maintained that it only collected geolocation data “with the express consent of the user.” (A true and accurate copy of Microsoft’s Letter to Congress, dated May 9, 2011, is attached hereto as **Exhibit A**.) Nevertheless, and in clear contradiction to its assertions, Microsoft designed its camera application to regularly transmit its users’ geolocation information to Microsoft’s servers—even when the user expressly denied Microsoft access to such information.

7. In September of 2011, shortly after this lawsuit was filed, Microsoft publicly admitted that its software continued to transmit users’ geolocation information without consent.¹ Microsoft has since deployed a software upgrade, Windows Phone 7.5, which purports to remedy

¹ Location and my privacy FAQ, <http://www.microsoft.com/windowsphone/en-US/howto/wp7/web/location-and-my-privacy.aspx> (last visited October 12, 2011).

1 the unlawful tracking at issue.

2 8. Rather than owning up to its deceptive behavior, Microsoft astonishingly claims
3 that this unlawful tracking was the result of a “bug” in its software.

4 9. The truth, however, is that Microsoft intentionally designed its Windows Phone
5 camera application to thwart consumers’ ability to prohibit the collection of their geolocation
6 information, in blatant disregard of its users’ privacy rights and federal law.

7 **PARTIES**

8 10. Plaintiff Rebecca Cousineau is a natural person domiciled in the State of
9 Michigan.

10 11. Defendant Microsoft Corporation is a Delaware corporation with its principal
11 place of business located at 1 Microsoft Way, in the City of Redmond, State of Washington.

12 **JURISDICTION AND VENUE**

13 12. This Court has jurisdiction over the subject matter of this action pursuant to 28
14 U.S.C. § 1331. This Court has personal jurisdiction over Defendant because it resides in this
15 District, conducts business in this District, and the improper conduct alleged in this Complaint
16 occurred in this District.

17 13. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant
18 resides in this District, conducts business in this District, the improper conduct alleged in this
19 Complaint occurred in this District, and the injury arose in this District. Venue is additionally
20 proper because Defendant transacts significant business in this District.

21 **FACTUAL BACKGROUND**

22 **I. Microsoft Profits from Collecting its Users’ Location Data**

23 14. Mobile advertising is projected to become a \$2.5 billion dollar industry by 2015.²
24 To gain a competitive advantage, Microsoft is using mobile devices running the Windows Phone
25 OS to build a digital map, comprised of cell tower and wireless network (“WiFi”) access point

26 _____
27 ² See, <http://www.nytimes.com/2011/04/26/technology/26locate.html> (last visited October 13, 2011).

1 information. (Ex. A, p. 4.) In turn, this map can be used to help pinpoint the location of users'
2 mobile phones and other devices.

3 15. In the future, Microsoft will be able to use its proprietary database of cell tower
4 and WiFi information to deploy targeted advertisements to mobile phone users based upon their
5 geolocations.

6 16. In order to gather the information for the database described above, Microsoft
7 designed the Windows Phone OS to collect and send geolocation data to its servers when "a
8 user-authorized application has made a request for location." (Ex. A, p. 4.)

9 17. However, when consumers used certain Windows Phone OS mobile applications,
10 they—regardless of their privacy restrictions—unwittingly transmitted specific geolocation data
11 to Microsoft.

12 18. Previously, Microsoft allowed public access via the Internet to its database
13 containing the approximate locations of millions of mobile phones, laptop computers, and other
14 devices that was gathered through, *inter alia*, its users' mobile devices.

15 19. Despite Microsoft's adamant claims to the contrary, researchers were able to
16 show that it was possible to track the approximate whereabouts of individual consumers using
17 information gleaned from Microsoft's database.³ Facing increased scrutiny over privacy
18 concerns raised by the researchers' discovery, Microsoft ceased publication of the contents of its
19 geolocation database.

20 **II. Microsoft Promises Not to Collect Geolocation Data Without User Consent**

21 20. In April of 2011, leaders of the United States House of Representatives
22 Committee on Energy and Commerce sent a letter to Microsoft requesting information about
23 how its software was designed to track and store users' locations. In its response to Congress's
24 inquiry, Microsoft unequivocally stated that the Windows Phone OS never collects geolocation
25 data without the express consent of its users. (Ex. A, pp. 1, 2, 4, 5, 9.)

26 _____
27 ³ See, Microsoft Curbs Wi-Fi Location Database, http://news.cnet.com/8301-31921_3-20086489-281/microsoft-curbs-wi-fi-location-database/ (last visited October 14, 2011).

21. Specifically, Microsoft asserted that its OS will “collect data *only* if ... the user has allowed an application to access and use location data.” (Ex. A, p. 4 (emphasis added).)

22. Microsoft’s representations to Congress were false.

III. Microsoft Intentionally Broke its Promise to Consumers

23. Through her attorneys, Plaintiff has retained an independent security expert to investigate whether Microsoft collected location information from Windows Phone users without consent. (A true and accurate copy of the Windows Phone 7 Geolocation Investigative Report (the “Report”) is attached hereto as **Exhibit B**.)

24. The research detailed in the Report shows that, even after a Windows Phone user expressly denied Microsoft access to location information through the camera application, the device transmitted the following data to Microsoft’s servers when the camera was activated: the approximate latitude and longitude coordinates of the user’s device, a unique identifier for the device, current date and time, and the locations of the closest cellular tower and WiFi network. (Ex. B, p. 4.)

25. As a result, Microsoft—and anyone else with access to this data—was provided with the exact location of hundreds of thousands of United States consumers who explicitly denied Microsoft access to such information.

IV. Microsoft Admits To Unlawful Tracking

26. In September of 2011, shortly after this lawsuit was filed, Microsoft issued a press release indicating that it had discovered a “bug” in its Windows Phone OS that caused mobile devices running the software to transmit location information to Microsoft’s servers through its camera application—without user consent.

27. Specifically, Microsoft’s press release stated, in relevant part, that:

We have identified an unintended behavior in the Windows Phone 7 software that results in information about nearby Wi-Fi access points and cell towers being periodically sent to Microsoft when using the Camera application ... the software bug results in the behavior even where you have disabled geo-tagging photos in

the Camera application.⁴

28. Although Microsoft attempts to blame its unauthorized tracking scheme on a software “bug,” the true facts show otherwise. Microsoft is one of the largest and most renowned software developers in the world, with a highly sophisticated staff of engineers. The idea that, during the programming process, these software engineers simply “overlooked” the fact that their own code was designed to ignore users’ refusal to consent to be tracked is simply untenable.

29. Furthermore, as described above, Microsoft made very specific representations to members of Congress about the functionality of its Windows Phone 7 OS that the Company now claims is flawed. Even assuming, *arguendo*, that Microsoft’s initial oversight led to the unlawful transmission of its users’ geolocation data, surely Microsoft’s engineering team conducted further investigation into the software before submitting to Congress that its software never transmits geolocation data without express permission of the user.

30. In truth, this was no coding error. Microsoft intentionally programmed its software to send its users’ geolocation information to its servers without consent because it wanted to maximize the amount of data it receives for use in its database. Now that it has been exposed, Microsoft is attempting to cover-up its malfeasance.

FACTS RELATING TO PLAINTIFF

31. In or around June 2011, Plaintiff Cousineau took ownership and possession of a new Samsung mobile device running the Windows Phone 7 operating system.

32. Cousineau first used the mobile device’s camera application in or around June 2011 and, when prompted by the camera application whether to allow access to her “location information,” Cousineau expressly denied the request by clicking “cancel.” (*See* ¶ 4.)

33. Undeterred, Microsoft ignored Cousineau’s express denial and intentionally recorded, on a frequent basis, the approximate latitude and longitude coordinates of her device, the unique identifier for her device, the date and time of the recording, and the locations of the

⁴ *See supra* note 1.

1 closest cellular tower and WiFi network.

2 **CLASS ALLEGATIONS**

3 34. **Definition of the Class:** Plaintiff Cousineau brings this action pursuant to Fed. R.
4 Civ. P. 23(b)(2) and (3) on behalf of herself and a Class of similarly situated individuals, defined
5 as follows:

6 All persons in the United States who, prior to August 31, 2011, denied their
7 Windows Phone 7 camera application access to their location information, and
unwittingly had their geolocation data transmitted to Microsoft's servers.

8 Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents,
9 successors, predecessors, and any entity in which the Defendant or their parents have a
10 controlling interest and their current and former employees, officers, and directors, (2) the Judge
11 to whom this case is assigned and the Judge's immediate family, (3) persons who execute and
12 file a timely request for exclusion, (4) the legal representatives, successors, or assigns of any
13 such excluded person, and (5) all persons who had claims similar to those alleged herein finally
14 adjudicated or who have released their claims against Defendant.

15 35. **Numerosity:** The exact number of the members of the Class is unknown and is
16 not available to Plaintiff at this time, but individual joinder in this case is impracticable. The
17 Class consists of tens of thousands of individuals and other entities. Class members can be easily
18 identified through Defendant's records and public records.

19 36. **Commonality:** There are many questions of law and fact common to the claims
20 of Plaintiff and the other members of the Class, and those questions predominate over any
21 questions that may affect individual members of the Class. Common questions for the Class
22 include but are not limited to the following:

23 (a) Whether Microsoft collected geolocation data through the camera
24 application included in the Windows Phone 7 operating system after the
25 user denied Microsoft access to that information;

26 (b) Whether Microsoft profits, or intends to profit, from the collection of
27

geolocation data obtained as a result of the unlawful practices described herein; and

(c) Whether Microsoft's conduct described herein violates the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*

37. **Typicality:** The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Class are the same and resulted in injury to Plaintiff and all of the other members of the Class. Plaintiff and the other members of the Class have all suffered harm as a result of Defendant's wrongful conduct.

38. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiff has no interests antagonistic to those of the other members of the Class and Defendant has no defenses unique to Plaintiff.

39. **Predominance and Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, since joinder of all members is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by the actions of Defendant. It would be virtually impossible for the individual members of the Class to obtain effective relief from the misconduct of Defendant. Even if members of the Class themselves could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

40. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to

the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole. The policies of the Defendant challenged herein apply to and affect all members of the Class uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct, not on facts or law applicable only to Plaintiff.

FIRST CAUSE OF ACTION

Violations of the Stored Communications Act 18 U.S.C. §§ 2701, *et seq.* (On behalf of Plaintiff and the Class)

41. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

42. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...." 18 U.S.C. § 2510(12). The Stored Communications Act (the "SCA") incorporates this definition.

43. Pursuant to the ECPA and the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their intended recipient.

44. The SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701.

45. Congress expressly included provisions in the SCA to address this issue so as to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99-541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

46. Microsoft programmed its Windows Phone 7 operating system to temporarily store the location information ("the stored file") of its users without their consent. Microsoft has

1 violated 18 U.S.C. § 2701(a)(1) because it intentionally accessed, and continues to access,
 2 consumers' communications without authorization and obtained, altered, or prevented authorized
 3 access to a wire or electronic communication while in electronic storage by collecting location
 4 data from the stored file on Plaintiff's and the Class's mobile devices through the camera
 5 application, despite the fact that the users expressly denied Microsoft access to that information.
 6 At all relevant times, Microsoft had actual knowledge of, and benefited from, this practice.

7 47. Additionally, Microsoft has violated 18 U.S.C. § 2701(a)(2) because it
 8 intentionally exceeded the authorization of consumers to access consumers' communications and
 9 obtained, altered, or prevented authorized access to a wire or electronic communication while in
 10 electronic storage by collecting location data from the stored file on Plaintiff's and the Class's
 11 mobile devices through the camera application, despite the fact that the user expressly denied
 12 Microsoft access to that information. At all relevant times, Microsoft had actual knowledge of,
 13 and benefited from, this practice.

14 48. As a result of Microsoft's conduct described herein and its violation of § 2701,
 15 Plaintiff and the other Class members have suffered injuries. Plaintiff, on her own behalf and on
 16 behalf of the Class, seeks an order enjoining Microsoft's conduct described herein and awarding
 17 herself and the Class the maximum statutory and punitive damages available under 18 U.S.C. §
 18 2707.

19 **PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiff Rebecca Cousineau, individually and on behalf of the Class,
 21 prays for the following relief:

22 A. Certify this case as a class action on behalf of the Class defined above, appoint
 23 Rebecca Cousineau as class representative, and appoint her counsel as class counsel;

24 B. Declare that Microsoft's actions, as described herein, violate the Stored
 25 Communications Act, 18 U.S.C. §§ 2701, *et seq.*;

26 C. Award injunctive and other equitable relief as is necessary to protect the interests
 27 of the Plaintiff and the Class, including, *inter alia*: an order prohibiting Microsoft from engaging

1 in the wrongful and unlawful acts described herein;

2 D. Award damages, including statutory damages under the Stored Communications
3 Act, 18 U.S.C. § 2707(c), and punitive damages where applicable, to Plaintiff and the Class in an
4 amount to be determined at trial;

5 E. Award Plaintiff and the Class their reasonable litigation expenses and attorneys'
6 fees;

7 F. Award Plaintiff and the Class pre- and post-judgment interest, to the extent
8 allowable; and

9 G. Award such other and further relief as equity and justice may require.

10 **JURY TRIAL**

11 Plaintiff demands a trial by jury for all issues so triable.

12 Dated: April 9, 2013

Respectfully submitted,

13 REBECCA COUSINEAU, individually on her
14 own behalf and on behalf of all others similarly
15 situated,

16 By: /s/ Ari J. Scharg
One of Plaintiff's Attorneys

17 Jay Edelson*
18 Rafey S. Balabanian*
19 Ari J. Scharg*
Chandler R. Givens*
EDELSON LLC
350 North LaSalle, Suite 1300
20 Chicago, Illinois 60654
21 Telephone: (312) 589-6370
22 Facsimile: (312) 589-6378
jedelson@edelson.com
23 rbalabanian@edelson.com
24 ascharg@edelson.com
cgivens@edelson.com
25 *Admitted *pro hac vice*

26 Kim D. Stephens, WSBA #11984
27 Janissa A. Strabuk, WSBA # 21827

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
kstephens@tousley.com
jstrabuk@tousley.com

*Counsel for Rebecca Cousineau and the Putative
Class*

CERTIFICATE OF SERVICE

I, Ari J. Scharg, an attorney, hereby certify that on April 9, 2013, I served the above and foregoing ***Plaintiff's Third Amended Class Action Complaint***, by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Ari J. Scharg